REMARKS

This Amendment is submitted in response to the Office Action dated March 22, 2006, having a shortened statutory period set to expire June 22, 2006. Proposed amendments to the Claims include **amending** Claims 1, 3, 5-6, 8, 10-11, 13 and 15, **cancelling** Claims 2, 4, 7, 9, 12 and 14, and **adding** Claims 16-21. Upon entry of the proposed amendments, Claims 1, 3, 5-6, 8, 10-11, 13 and 15-21 will now be pending.

Applicants appreciate the time and courtesy extended by Examiner Stoynor and Supervisor Browne during a June 21, 2006 teleconference. An agreement was reached that Claim 1, as presently amended to include the features of original (and now cancelled) Claim 4, is not taught or suggested by the cited prior art. If Applicants' undersigned representative has misunderstood this agreement, telephonic notification at the Examiner's earliest convenience would be greatly appreciated.

Objection to the Specification

On Page 2 of the present Office Action, the Examiner has objected to the lack of serial numbers for co-pending applications. These numbers are now found in the present amendment, and thus the objection should be removed.

Similarly, the Examiner has objected to the use of "computer usable medium" instead of "signal-bearing media." While Applicants respectfully traverse this objection, the specification is presently amended in conformance with the suggestion of the Examiner. No new matter is added by this amendment.

Double Patent Rejection

On Page 2 of the present Office Action, the Examiner has presented a non-statutory obviousness-type double patenting rejection against co-pending U.S. Patent Application Nos.

10/674,776, 10/698,207 and 10/698,128. Appropriate terminal disclaimers are enclosed herein, and thus this rejection should be withdrawn.

Rejection under 35 U.S.C. § 103

On Page 5 of the present Office Action, Claims 1-15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Zimmer et al.* (U.S. Patent Application Publication No. 2004/0193867 – "*Zimmer*") in view of *Schell et al.* (U.S. Patent No. 6,314,520). Applicants respectfully traverse these rejections.

With regards to exemplary **Claim** 1, the combination of the cited art does not teach or suggest "storing, under a control of a remote management computer that is connected to a client computer, a list of trusted configuration servers in a Remote Supervisor Adapter (RSA) card on the client computer", as supported in the present specification at paragraph [0016]. While the cited art references a Network Interface Card (NIC), the combination of the cited prior art does not teach or suggest the use of an RSA card. Exemplary **Claim 17**, which is supported by paragraph [0016] of the present application, is added to clarify the feature that the remote management computer is performing the storing of the list of trusted configuration servers in an RSA card on the client computer.

Zimmer is cited for teaching that a server can be securely connected to a client to download boot images (*Zimmer* Figures 1 and 4). Examiner notes that *Zimmer* fails to disclose storing a list of trusted configuration servers in the client computer. However, at col. 2, lines 30-35, col. 3, liens 6-11, col. 4 line 64 to col. 5, line 2, and col. 5, lines 13-22, *Schell* teaches that a NIC can store addresses of trusted servers, which are compared to the source address of incoming packets.

The Examiner's position, as understood by the Office Action and the June 21, 2006 teleconference, is essentially that *Zimmer* teaches that a server can control a client, *Schell* teaches that a client computer can store a list of trusted servers in the client computer's NIC, so therefore the combination teaches that a secure server can store the list of trusted computers in the client computer.

Consider now *Schell* at col. 6, lines 8-20:

> "Initialization continues with step 124 wherein the CPU executes the program instructions resident in the NIC BIOS 65 (FIG. 3) to initialize the hardware in the NIC. Following hardware initialization, the CPU downloads the pre-boot modules from the server in step 126 and in step 128, executes these pre-boot modules to perform the identification and authorization function associated with the login process described in FIG. 6. In addition the CPU loads the registers of the NIC's send address confirmation circuitry 66 and the receive address confirmation circuit 88 (FIG. 3) with values stored in the NIC BIOS ROM. In an alternative embodiment, the pre-boot modules may be stored in the NIC BIOS." (emphasis added)

As stated in Section 2143.03 of the MPEP, it is axiomatic that the prior must teach or suggest every claim limitation. Neither *Schell* nor *Zimmer* teaches a supervisory computer storing a list of trusted configuration servers in the client computer. The combination of *Zimmer* (a supervisory computer) with *Schell* (a client computer loading the list in a NIC) does not teach or suggest the limitation of the supervisory computer storing the list in the client. That is, the combination of the cited art teaches that the information as to which server is to be trusted comes NOT from a remote supervisory computer, but from the client computer itself (i.e., from the client computer's NIC BIOS). There is no suggestion that the storage of such a list may come from, and be under the control of, a remote supervisory computer. The fact that a server can control a client does not teach or suggest the scenario in which the remote supervisory computer performs the storing of the list of trusted configuration servers in the client computer.

Furthermore, the combination of the cited art does not teach or suggest "in response to determining that the responding configuration server is not on a list of trusted configuration servers, selecting, by the client computer, a selected server from one of the servers on the list of trusted configuration servers; and requesting, by the client computer, the configuration parameters from the selected server," as supported in the present specification by Figure 3, blocks 318 and 308.

Schell is cited for teaching the discarding of packets that are from untrusted locations, and accepting only packets from trusted locations. There is no teaching or suggestion of getting a configuration parameter from a server that is selected from the list of trusted configuration servers. That is, *Schell* examines the source address of incoming packets, while Claim 1 relates to the client computer choosing a server to make a call to.

With regards to exemplary **Claim 3**, the combination of the cited art does not teach or suggest "upon determining that the responding configuration server is not on the list of trusted configuration servers, generating an alert...of an unauthorized configuration server." *Zimmer* is cited at paragraph [0044] for teaching this feature. However, *Zimmer* teaches sending a message to an administrator if no boot option offers were received. Claim 3 is directed to sending a message to an administrator if the responding configuration server is not on the trusted list. While the client computer may end up in the same condition (not getting a boot), teaching a possible result is not the same as teaching a limitation.

Regarding exemplary new **Claim 16**, the cited art does not teach or suggest "wherein the remote management computer is a part of an Information Technology (IT) services organization that manages various types of Pre-boot eXecution Environment (PXE) deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer," as supported in paragraph [0021] of co-pending U.S. Patent Application No. 10/674,776 (which has been incorporated by reference by the present application).

PAGE 12/16 * RCVD AT 6/22/2006 10:40:01 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/10 * DNIS:2738300 * CSID:5123436446 * DURATION (mm-ss):05-18

CONCLUSION

For the reasons stated above, Applicants now respectfully request a Notice of Allowance for all pending claims.

Applicant further respectfully requests the Examiner contact the undersigned attorney of record at 512.617.5533 if such would further or expedite the prosecution of the present Application.

No extension of time for this response is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application, including any required fees associated with the included Terminal Disclaimers, to **IBM CORPORATION DEPOSIT ACCOUNT No. 50-0563**.

Respectfully submitted,

James E. Boice
Registration No. 44,545
DILLON & YUDELL LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)